Wilton Park

Image: geralt

Conference report

Privacy, security and surveillance: tackling dilemmas and dangers in the digital realm

Monday 17 – Wednesday 19 November 2014 | WP1361

In partnership with: Institute for Human Rights and Business — Shaping Policy • Advancing Practice • Strengthening Accountability

With support from: ERICSSON; REGERINGSKANSLIET Ministry for Foreign Affairs Sweden; VimpelCom

Wilton Park

Conference report

Privacy, security and surveillance: tackling dilemmas and dangers in the digital realm

Monday 17 – Wednesday 19 November 2014 | WP1361

Introduction

The Wilton Park conference brought together international experts from government, business and civil society to discuss the challenges of privacy, security and surveillance in the digital realm and to explore possible ways forward. The discussion included export control, mass surveillance and the challenges business operations face in high-risk countries.

The relationship between national security and the privacy and human rights of individuals is complex. A vigorous debate has been prompted by the June 2013 release of documents by former US National Security Agency (NSA) contractor Edward Snowden, revealing the methods by which intelligence agencies in the UK and the US gathered, collected and shared data.

These revelations have raised fundamental questions about privacy and security in many fora. There are strong views among government, business and civil society about the application of measures to ensure safety and security and protect privacy in the digital realm.

The rights to security and privacy are intertwined. It can be argued that there is no respect for human rights in the absence of a secure society, and no security without respect for human rights. Governments have a duty to protect citizens from terrorism and other threats, but in so doing the utmost care should be taken to ensure that fundamental freedoms are not compromised. Where they are circumscribed, such acts should be legal, temporary, and overseen by appropriate authorities accountable to the public.

This debate is important and timely. Technological advancements to facilitate increased communications are fast moving, with industry undergoing rapid digital transformation. The amount of data collected, stored and available is growing exponentially and states are attempting to keep pace with change. Vast quantities of information are now stored in the "cloud," under the control of private and sometimes public corporations. This is often without clear lines of authority and responsibility, governing who has access to the data and for what reason.

There is an urgent need to address the issue of data collection and retention by governments and companies. Legal frameworks should ensure that individuals know what information is being collected and what it is used for. Where surveillance is authorised, there should be clarity regarding the rules that govern the process. Furthermore, the laws governing interception and surveillance require effective oversight. In cases where these tools are misused, either intentionally or otherwise, there should be redress and remedy. The expectations and responsibilities of companies in the information and communication technology (ICT) sector, in relation to both users and governments, should be examined as a matter of priority.

Key issues:

” It is unreasonable to assert that users of digital communications have automatically forfeited their right to privacy”

- A division of the world into “good” and “bad” countries is unhelpful and should be avoided. Human rights are universal and international standards, in particular peremptory norms, apply to all states. Every state has the obligation to respect, protect and fulfil human rights. On the other hand, there is a clear demarcation between “open” and “closed” states and this distinction is a real one in the human rights and ICT debate.
- It is unreasonable to assert that users of digital communications have automatically forfeited their right to privacy. This is highlighted in reports by the former UN High Commissioner for Human Rights and the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. The UN reports also observe that the use of mass surveillance technology effectively undermines the right to privacy of communications on the internet.
- In the UK, there is not yet a definition of mass surveillance or bulk access of digital communications and the law regarding bulk data collection and storage by the intelligence agencies is unclear. Large scale interception or surveillance of private communications should be in the public interest and proportionate to the threat. However, proportionality cannot be tested in the absence of a public justification of the operation; without transparency, public oversight cannot be meaningful.
- While the discussion on surveillance and appropriate oversight is taking place in the US and Europe, there are many countries where there is no public dialogue. In many states there is neither the political will nor safe space for stakeholders to debate the issues freely. However, open discussions about surveillance reform and oversight in Europe and the US could have a positive influence on the global discourse.
- Surveillance technologies created and manufactured in Europe have been used by governments with a poor record on human rights. The cost of conducting surveillance and collecting data has fallen and the technology is now more accessible and affordable. As a result, more states now have the technical capability to conduct surveillance- a power which few countries are likely to rescind.
- It is widely felt that export controls and regulations governing the sale of surveillance technology are being outpaced by technological developments. National and regional bodies, including the European Union, will need to act swiftly in order to update regulations governing surveillance exports.

“…more states now have the technical capability to conduct surveillance…”

- Companies and governments need to be more transparent. There is a view that corporate transparency reporting could be more effective and meaningful, and that governments should be consistent in releasing transparency reports.
- Governments developing an effective multidisciplinary approach to address surveillance, privacy and human rights should include the judiciary, parliamentarians, technologists, corporations, and the human rights community.

Context and challenges for governments

1. Surveillance powers in the UK have generated much discussion in recent months. The Regulatory Investigatory Powers Act (RIPA) of 2000 is a key piece of legislation governing surveillance in the UK. Part 1 of the Act (which deals both with interception and communications data) is currently undergoing review. The Snowden revelations and resultant litigation have raised public awareness of the application of powers under the Act. There is a view that the UK Government would not have revisited these powers had it not been for Snowden and the April 2014 judgement of the European Court of

Justice. The ruling declared the European Commission Data Retention Directive invalid thereby invalidating UK regulations mandating data retention by communications providers.

2. The introduction of the Data Retention and Investigatory Powers Act (DRIPA) on an emergency timetable is seen as a response to the European ruling. The accompanying conditions include an independent review of the new Act and of the RIPA.

"Legal procedures should be subject to proper scrutiny and legislative processes, open and accountable through parliamentary debate."

3. The UK's definition of mass surveillance is much debated. It is argued that bulk access of digital communications constitutes mass surveillance and is therefore a violation of privacy. Others argue that the act of bulk access or bulk data collection is being carried out by a machine programmed to discard irrelevant data and therefore does not constitute surveillance: arguably surveillance only occurs when information is being viewed by a human being.

4. Bulk access to digital communications can be seen as a direct challenge to Article 17 of the ICCPR (the right to privacy). Targeted surveillance depends on prior suspicion and, in the UK, requires executive prior authorisation. Under British law, all warrants signed to permit lawful interception should meet the test of proportionality. It is argued that mass surveillance/bulk access cannot meet the proportionality test. Assertions by the intelligence services that bulk collection contributes to counter-terrorism strategy should not therefore be regarded as a legal justification. Legal procedures should be subject to proper scrutiny and legislative processes, open and accountable through parliamentary debate.

5. There is an important distinction between communications data and content, governed by two separate authorisation regimes in the UK. Agencies can obtain communication data through self-authorisation dependent on internal checks and balances. However, access to the content of communications, requires proper authorisation in the form of a warrant signed by the Home Secretary. Data encryption has made it more difficult for intelligence agencies to access the content of messages and calls. At the same time, considerable metadata is available from "apps" and electronic devices, through location information and "cookies" which companies retain. In another example, the content of a journalist's communications becomes public when the article is published, however the information source may be confidential. There are concerns that access to communications data may allow intelligence agencies to identify journalistic sources.

"…under some circumstances, the agencies should go beyond the NCND default, in order to ensure meaningful accountability"

6. In general, the intelligence agencies respond to queries of this nature by neither confirming nor denying (NCND). Whilst acknowledging the need to keep some information secret eg operational activities and the identity of agents, there is a view that, under some circumstances, the agencies should go beyond the NCND default, in order to ensure meaningful accountability.

7. The distinction between internal and external communications is an important one in that the classification impacts the grounds by which interception can be used under RIPA. This has implications for governments and for business.

8. The role and remit of the security apparatus is much debated. Who is it designed to serve: should it be affording protection to non-citizens as well as citizens? And how does this align with international human rights law founded on the premise that all persons should enjoy human rights without discrimination.

9. Global practice regarding privacy protection for nationals and non-nationals and for those within and outside state jurisdiction is inconsistent and the legal obligations of states are unclear.

10. The issue of extraterritorial enforcement is to be explored through the work of the UK's recently appointed Special Envoy on intelligence and law enforcement data sharing.

11. Some countries have robust statutory oversight of intelligence agencies, however this needs to be underpinned by effective framing, interpretation and implementation of the rules on interception. The data flowing through networks will continue to increase, as

"In the worst case scenario, bulk access of digital communication could result in repeated tapping of data on a global basis"

will the ability to process, sift, record and store this information. The nature of the Internet is such that multiple parties from a range of countries will be able to collect data on individuals. National laws designed to protect people within a country's jurisdiction will apply to some agencies but may not constrain all actors, including non-state. In the worst case scenario, bulk access of digital communication could result in repeated tapping of data on a global basis.

The Impact of the Surveillance Debate Outside Europe and the USA

12. There is discourse in the United States and Europe about the role of intelligence agencies, surveillance, and the relationship with the private sector. However, there are regions of the world where this discussion is not possible and many governments do not engage in the debate.

"The discussion on surveillance and privacy should be seen in the context of wider threats to freedom of expression"

13. The UK is engaged in discussion regarding the reform of RIPA. In comparison, there are countries that do not have oversight or appropriate checks and balances; in some cases, there are no legal provisions at all. Lawful interception is based on lawful authority. However, laws in many jurisdictions may be inconsistent with international standards.

14. The discussion on surveillance and privacy should be seen in the context of wider threats to freedom of expression in many parts of the world. State and corporate control can include network disconnection and other censorship practices, such as blocking or removing content from the web in order to curb dissent.

Context and challenges for business

"...in some countries almost 50% of GDP flows through mobile money transfers…"

15. Business needs to ensure respect for customer privacy in order to maintain the trust of service users. It is also in a company's commercial interest to enable communication: the more people transmit data, the better it is for businesses. However, there has been a reduction in the level of trust in ICT companies.

16. It is argued that the increased collection of user data by companies will prompt intelligence agencies to want greater access. What limits are companies setting so that they do not collect unnecessary data? For example, in some countries almost 50% of GDP flows through mobile money transfers. Routine interception and tracking of transfers would expand surveillance capability beyond the capacity of current communications data.

17. The issue goes beyond ICT companies. Many industries are undergoing a digital transformation, increasingly relying on digital tools and features in products and services as a key component of business. This has increased access to consumer data for corporates who may not have appropriate protocols in place. Established ICT companies could play a role in educating the next generation of tech companies about the risks from a human rights perspective.

18. The surveillance capabilities of countries are increasing, as barriers to access and affordability decrease. Furthermore, the regulations governing export control of surveillance and related equipment are complex and classified on particular technical features, making the process difficult to follow. In addition to the export of sophisticated equipment, companies may provide installation, training and tailored services taking into account different infrastructures for overseas clients, all of which can have human rights implications.

Extraterritoriality

"Extraterritoriality is a key concern for business…"

19. Extraterritoriality is a key concern for business, particularly with regard to the complex routing of Internet communications and the classification of internal and external communications. For example, a warrant requesting access to a user's communications may be valid in the country of issue, but may conflict with laws in the home state of the company.

20. The extraterritoriality impact of DRIPA has not yet been put to the test in the UK. In the US, a case in the New York Second Circuit of Appeals concerns the dispute following a US warrant served on Microsoft ordering the company to produce user email content even though it was stored exclusively in Ireland. Microsoft argues that the US warrant does not compel the company to hand over data stored in a foreign jurisdiction. The judgement of this case could have global implications.

"…it is not possible to create a technological "back door" that could only be used by security agencies."

21. There is some reluctance to use Mutual Legal Assistance Treaty (MLATs), as they are cumbersome and slow. It is argued that the process could be improved if there was the political will to do so. There are concerns that some governments have obtained information from a company's servers without proper authorisation and that this has come about due to the slow process of MLATs and the use of technology, such as spyware, to bypass MLATs altogether. There is a strong view that it is not possible to create a technological "back door" that could only be used by security agencies. This entry point would be vulnerable to exploitation by other governments, criminals or other non-state actors.

Context and challenges for civil society

"…the case against the Zero 9 bloggers in Ethiopia includes the evidence that they received training on encryption tools…"

22. The space for civil society to act has been shrinking. Laws are being passed in some countries to curb the activities of NGOs and activists. Civil society groups also face resource limitations: these constraints are not just financial, but also technical and many groups need technical assistance and training. In many cases, the personal security of individuals is under constant threat.

23. In order to secure their communications, several civil society groups have chosen to encrypt. However, some governments view this with suspicion. For example, one of the charges in the case against the Zero 9 bloggers in Ethiopia includes the evidence that they received training on encryption tools and that they had reached out to international NGOs for advice.

24. There are differing views on privacy rights: some governments believe that these rights are not infringed unless the data is reviewed by a human being. It is also suggested that civil society should test if data collection causes any harm. Research from Human Rights Watch[1] has found that some writers and journalists are self- censoring their work due to concerns that they may be under surveillance. There are indications that this practice is not confined to non-democratic countries. Human rights groups have noted the impact on journalists whereby some sources are unwilling to speak or be approached, as they fear discovery.

"…some writers and journalists are self-censoring their work due to concerns that they may be under surveillance."

25. It is challenging to demonstrate the harm of data collection on individuals: there are relatively few cases by which academics and civil society groups concerned with privacy and other human rights are able to illustrate the serious impact surveillance can have on the public. For example, the phone-hacking case in the UK prompted limited public outcry to the revelation that a number of celebrities' voicemails were hacked by tabloid journalists. Public opinion changed to outrage when it emerged that the voicemail of murdered schoolgirl Milly Dowler had also been hacked.

Improving transparency

26. Transparency is a key component of transactions based on trust: companies and governments should be able to assure citizens that their data is secure. In Estonia, the identity of the individual is core to online security. The government is the guarantor of online transactions and citizens give their consent for different organisations to access their data. Estonian citizens can view online lists indicating who has accessed different databases with their personal information. Unauthorised access is investigated and

[1] Human Rights Watch (2014) *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy* Available at: http://www.hrw.org/reports/2014/07/28/liberty-monitor-all

"Many laws regarding surveillance are opaque and states are increasingly requesting direct access to networks"

citizens are guaranteed redress in order to maintain the relationship of trust.

27. Many laws regarding surveillance are opaque and states are increasingly requesting direct access to networks. Companies that aspire to transparency through statistical reporting of such requests are sometimes prevented by law from publishing this information.

28. Given that the general public remains largely unaware of surveillance laws and capabilities, companies can play a role in addressing the asymmetry of information. The Vodafone Law Enforcement Disclosure Report[2] is a good example, in that it outlines relevant laws in different jurisdictions. A logical next step would be for companies to advise users of government requests for access to their data.

29. It has been proposed that more governments could issue transparency reports. However, companies have commercial drivers regarding their relationship with users that do not apply to governments in the same way. Government dialogue on surveillance is largely driven by security concerns including anti-terrorism policies.

30. It is difficult to compare transparency reports: governments and corporates calculate and record statistics in different ways. This disparity means, for example, that the aggregated statistics of all company reports may not equal the figure of government requests. Consistency of recording is essential for clarity and transparency as well as effective policy development.

" …best practice is embodied by a robust oversight mechanism that includes strong investigatory powers, democratic accountability and the availability of redress."

What does best practice look like?

31. In the view of many, best practice is embodied by a robust oversight mechanism that includes strong investigatory powers, democratic accountability and the availability of redress. Among the models regarded as noteworthy is the best practice compilation in the 2010 report by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism[3]. The rules and regulations governing lawful interception in Croatia have been singled out as a good example, as has the oversight mechanism in Canada. The Netherland's intelligence oversight body, Commissie van Toezicht betreffende de Inlichtingen-en VeiligheidsDiensten (CTIVD) published a report[4] on the processing of telecommunications data in 2013, is also well regarded.

32. The International Principles on the Application of Human Rights to Communications Surveillance (known as the Necessary and Proportionate Principles[5]), endorsed globally in May 2014 by 500 civil society organisations, elected officials and political parties and academics are cited as another example of good practice.

33. Following the UN Resolution, adopted in 2013, on the right to privacy in the digital age[6], the chief sponsors of that resolution, Brazil and Germany, proposed a new text, which

[2] Available at: http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

[3] A/HRC/14/46 17th May 2010 *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight.* Available at: http://www.dcaf.ch/content/download/73465/1123242/version/1/file/A_HRC_14_46_english.pdf

[4] Available at: http://www.ctivd.nl/?download=Report 38 processing telecommunications data.pdf

[5] Available at: https://en.necessaryandproportionate.org/

[6] A/RES/68/167 18th December 2013 http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

was adopted in November 2014 (subsequent to the Wilton Park conference[7]). It states that the legal framework of surveillance should be clear and publicly accessible, refers to the interception of metadata as a highly intrusive act, and recommends that individuals whose right to privacy has been violated by surveillance should have access to remedy. The resolution also asks the UN Human Rights Council to consider appointing a UN Special Rapporteur on the Right to Privacy.

"There are concerns that international companies operating overseas do not always apply international standards"

How can a company use its leverage effectively?

34. The UN Guiding Principles for Business and Human Rights call upon companies to use their leverage to improve the human rights situation where they operate. In some cases, this may mean that a company should withdraw from the country and there is much debate about the circumstances that would trigger this decision. In general, business people will assert that the technology brings about significant economic and societal benefits and therefore companies should stay and engage. Withdrawal from a country is unlikely to resolve the human rights situation and positive transformation is more likely if companies remain engaged and push for reform.

35. There are concerns that international companies operating overseas do not always apply international standards. Corporates operating in Africa and Central Asia have been particularly criticised. In response, business representatives say that they are often constrained due to the risk to operating licenses and to staff on the ground. In some countries, if the company does not comply with government requests, there may be legal or other consequences for senior management and staff, including threats of imprisonment. International companies appear to have greater leverage: there are a number of examples whereby a refusal to comply with state requests has been followed by a legal challenge to the government. National companies are less likely to take this course of action.

36. The UN Guiding Principles on Business and Human Rights provide a common language and standards by which all stakeholders can discuss the issues. There is a general view that new guidelines are unnecessary and that the focus should be on the implementation of existing frameworks and ways in which they can be applied, calling business to account regarding their human rights policies and processes. The Guiding Principles assist civil society to ask specific questions about how a company identifies and assesses risk. They also provide a framework by which a company can structure the response.

"The UN Guiding Principles on Business and Human Rights provide a common language and standards"

37. Human rights impact assessments need to be confidential, however verification of the assessment by a third party would do much to legitimise the process. For example, members of the Global Network Initiative (GNI) members could be engaged: they already undergo third party assessment on the implementation of GNI's Principles.

38. The Freedom Online Coalition could play a role in helping members draft appropriate laws regarding interception of communications.

Proposed policy recommendations:

- Mass surveillance and bulk collection of data need to be defined.
- The criteria for permitting export of surveillance technology and equipment should change and be made consistent with states' human rights obligations and standards, and encompass up-to-date technology.
- Mutual Legal Assistance Treaty (MLAT) process should be reformed.
- Governments should explore the possibility of notifying people who have been surveillance targets after the fact.

[7] A/C.3/69/L.26/Rev.1 19th November 2014
http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/69/L.26/Rev.1

- Governments and companies who are not part of the current discussion need to be brought into the process as a matter of urgency.
- The Freedom Online Coalition can play a role in helping states draft laws governing surveillance and creating oversight bodies.
- The Freedom Online Coalition member-states should report recent internal debates regarding surveillance reform.
- Governments should consider issuing their own transparency reports.
- Transparency reports of companies should be standardised and methodology be developed to ensure that corporate and state figures align.

Lucy Purdon
Wilton Park | January 2015